CHAPTER 2

Notations and Preliminary results

2.1. Definitions and properties

For $\alpha \in \mathbb{Q}_p$, we can write $\alpha = p^r(a_0 + a_1 p + \cdots)$, where $a_i \in \{0, \cdots p-1\}$ for all i, $a_0 \neq 0$. In this section we will offer some preliminary results of $\mathbb{Q}_p$.

DEFINITION 2.1.1. Let F be a field. A map $|\cdot|\colon F \to \mathbb{R}$ is called a *norm* on F if the following conditions hold:

(1) $|x| \geq 0 \ \forall \ x \in F$ and $|x| = 0$ if and only if $x = 0$.

(2) $|xy| = |x||y|$.

(3) $|x + y| \leq |x| + |y|$.

We define a map $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}$ by $|a|_p = p^{-r}$ if $a = p^r(\sum_{i=0}^{\infty} a_i p^i)$, where $a_i \in \{0, \cdots p-1\}$ for all i, $a_0 \neq 0$. Then it easy to check $|\cdot|_p$ is a norm on $\mathbb{Q}_p$. Furthermore we have $|x + y|_p \leq \max\{|x|_p \, , |y|_p\}$. Under the norm $|\cdot|_p$ we let

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \, ; |a|_p \leq 1\}, M_p = \{a \in \mathbb{Q}_p \, ; |a|_p < 1\}.$$

Then $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$ with only one maximal ideal M_p. We called $a \in \mathbb{Z}_p$ a *p-adic integer*.

DEFINITION 2.1.2. Let K be an extension of F. A norm $|\cdot|_K$ on K is said extending $|\cdot|_F$ on F if $|a|_K = |a|_F$ for all $a \in F$.

LEMMA 2.1.3. *Let K be a finite extension of $\mathbb{Q}_p$. For any $\alpha \in K$ we define $|\alpha|_K = |N_{K/\mathbb{Q}_p}(\alpha)|_p^{\frac{1}{[K:\mathbb{Q}_p]}}$. Then $|\cdot|_K$ is the unique norm on K extending the norm $|\cdot|_p$ on $\mathbb{Q}_p$.*

Proof. See [2], Corollary 10 and Theorem 11. □

For $\alpha \in \mathbb{Q}_P^{alg}$, define $|\alpha| = |N_{K/\mathbb{Q}_p}(\alpha)|_p^{\frac{1}{[K:\mathbb{Q}_p]}}$ if $\alpha \in K$ for some finite extension K of $\mathbb{Q}_p$, then $|\cdot|$ is well-defined and extends $|\cdot|_p$ uniquely. Hence for convenience we replace $|\cdot|_K$ by $|\cdot|_p$.

Let K be a finite extension of $\mathbb{Q}_p$ of degree n, and let

$$O_K = \{\alpha \in K; |\alpha|_p \leq 1\}, M_K = \{\alpha \in K; |\alpha|_p < 1\}.$$

Then O_K is a ring, which is the integral closure of $\mathbb{Z}_p$ in K. M_K is its unique maximal ideal, and O_K/M_K is a finite extension of $\mathbb{F}_p(= \mathbb{Z}_p/M_p)$ of degree at most n. We called O_K/M_K (rep. $\mathbb{Z}_p/M_p$) the *residue field* of K (rep. $\mathbb{Q}_p$), denote it by $\overline{O_K}$ (rep. $\overline{\mathbb{Z}_p}$). We call [$\overline{O_K} : \overline{\mathbb{Z}_p}$] the *relative degree* of K.

For $a \in \mathbb{Q}_p$, if $a \neq 0$, write $a = p^r(\sum_{i=0}^{\infty} a_i p^i)$, where $a_i \in \{0, \cdots, p-1\}$ and $a_0 \neq 0$. Define a map $\upsilon_p : \mathbb{Q}_p \to \mathbb{Z}$ by $\upsilon_p(a) = n$, $\upsilon_p(0) = \infty$. Then for $a, b \in \mathbb{Q}_p$, υ_p satisfies

(1) $\upsilon_p(a) = +\infty \Leftrightarrow a = 0$,

(2) $\upsilon_p(ab) = \upsilon_p(a) + \upsilon_p(b)$,

(3) $\upsilon_p(a+b) \geq \min\{\upsilon_p(a),\ \upsilon_p(b)\}$.

Let F be a field, we call a map from F to $\mathbb{Z}$ satisfying these conditions a *discrete valuation* (we usually call it valuation for short) on F. On condition (3), it is easy to show that if $\upsilon_p(a) \neq \upsilon_p(b)$, then $\upsilon_p(a+b) = \min\{\upsilon_p(a),\ \upsilon_p(b)\}$.

An element $\pi \in O_F$ is said to be a *prime element* if $\upsilon(\pi)$ generates the group $\upsilon_p(F^*)$. For example, p is a prime element of $\mathbb{Q}_p$.

Let K be a finite extension of $\mathbb{Q}_p$. For $\alpha \in K$, define $\upsilon_K(\alpha) = -\log_p |\alpha|_p$, then υ_K is a valuation on K and $\upsilon_K(a) = \upsilon_p(a)$ for all $a \in \mathbb{Q}_p$.

In the following chapters we will sometimes use valuation to describe a finite extension of $\mathbb{Q}_p$, and sometimes use norm to do it.

DEFINITION 2.1.4. Let $[K : \mathbb{Q}_p] = n$ and υ_K, υ_p are valuations of K and $\mathbb{Q}_p$, respectively (for convenience we replace υ_K by υ_p in the following chapters). If we set $\upsilon_p(p) = 1$, then $\upsilon_K(K^*)$ is a subgroup of $(1/n)\mathbb{Z}$ with the form $(1/e)\mathbb{Z}$ for some $e \in \mathbb{N}$ and $e|n$. we call this e the *ramification index* of K. If $e = 1$, we say K is an *unramified* extension of $\mathbb{Q}_p$. If $e = n$, we say K is a *totally ramified* extension of $\mathbb{Q}_p$. If $p \nmid e$, we say K is a *tamely ramified* extension of $\mathbb{Q}_p$.

In the next lemma we have the relation between ramification index and relative degree of a finite extension of $\mathbb{Q}_p$.

LEMMA 2.1.5. *Let K be a finite extension of $\mathbb{Q}_p$ of degree n and e be the ramification index of K, f be the relative degree, then $n = ef$.*

Proof. See [**1**], Proposition 2.4. □

By this lemma we immediately get a conclusion : If K is a finite extension of $\mathbb{Q}_p$ of degree q, where q is a prime number, then $K/\mathbb{Q}_p$ is either unramified or totally ramified.

It is well-known that for every finite extension of $\mathbb{Q}_p$ we can find its maximal unramified subextension, and the extension can be obtained by adjoining a root to its maximal unramified subextension. In fact, the extension is totally ramified over its maximal unramified subextension. Hence we only need to discuss unramified and totally ramified extensions.

2.2. Unramified extensions of $\mathbb{Q}_p$

In this section, we will describe unramified extensions of $\mathbb{Q}_p$.

Let K be an unramified extension of $\mathbb{Q}_p$ with degree n and let $\overline{O_K} = \overline{\mathbb{Z}_p}(\theta)$ with $\theta \in \overline{O_K}$. Let $f(x)$ be a polynomial over $\mathbb{Z}_p$ such that $\overline{f}(x) = \mathrm{Irr}(\theta, \overline{\mathbb{Z}_p})$. Then $f(x)$ is irreducible over $\mathbb{Q}_p$ of degree n. Let α be a root of $f(x)$, then $K = \mathbb{Q}_p(\alpha)$. Conversely, given $f(x) \in \mathbb{Z}_p[x]$ such that $\overline{f}(x)$ is separable over $\overline{\mathbb{Z}_p}$, then we get an unramified extension by adjoining a root of $f(x)$. This conclusion is listed in theorem 2.2.2.

But in the proof of theorem 2.2.2 we first need to prove that if f(x) is irreducible over $\mathbb{Q}_p$, then $\overline{f}(x)$ is irreducible over $\overline{\mathbb{Z}_p}$. The following lemma offers some message we want to know.

LEMMA 2.2.1. (*Hensel's Lemma*). *Let $f(x)$ be a monic polynomial over $\mathbb{Z}_p$. If $\overline{f}(x) = g_0(x)h_0(x)$ in $\overline{\mathbb{Z}}_p[x]$, where $g_0(x)$ and $h_0(x)$ are relatively prime in $\overline{\mathbb{Z}}_p[x]$, then there exists monic polynomials $g(x)$, $h(x)$ in $\mathbb{Z}_p[x]$ such that $f(x) = g(x)h(x)$ and $\overline{g}(x) = g_0(x)$, $\overline{h}(x) = h_0(x)$ in $\overline{\mathbb{Z}}_p[x]$. In particular, let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial over $\overline{\mathbb{Z}}_p$ and let $f'(x) = na_n x^{n-1} + \cdots + a_1$ be the derivative of $f(x)$. Let β be an element in $\mathbb{Z}_p$ such*

that $f(\beta) \equiv 0 \pmod{p}$ *and* $f'(\beta) \not\equiv 0 \pmod{p}$. *Then there exists an unique* $\alpha \in \mathbb{Z}_p$ *such that* $f(\alpha) = 0$ *and* $\alpha \equiv \beta \pmod{p}$.

Proof. See [**1**, p.37] □

Now we can prove theorem 2.2.2.

THEOREM 2.2.2. *Let* $f(x)$ *be a monic polynomial over* $\mathbb{Z}_p$ *such that its residue is a monic separable polynomial over* $\overline{\mathbb{Z}_p}$. *Let* α *be a root of* $f(x)$ *in* $\mathbb{Q}_p^{alg}$. *Then the extension* $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ *is unramified.*

Proof. Let α be a root of $f(x)$ and let $f(x) = \prod_{i=1}^{n} f_i(x)$ be the decomposition of $f(x)$ into irreducible monic factors in $\mathbb{Q}_p[x]$. Furthermore we can make $f_i(x) \in \mathbb{Z}_p[x]$ and in fact $\alpha \in \mathbb{Z}_p$. Without lost of generality we can suppose α is a root of $f_1(x)$. By hypothesis we have $\overline{f_1}(x)$ is separable over $\overline{\mathbb{Z}_p}$. Lemma 2.2.1 implies $\overline{f_1}(x)$ is irreducible over $\overline{\mathbb{Z}_p}$. Let $\theta = \overline{\alpha}$, then

$$deg f_1(x) = [\, \mathbb{Q}_p(\alpha) : \mathbb{Q}_p \,] \geq [\, \overline{O_{\mathbb{Q}_p(\alpha)}} : \overline{\mathbb{Z}_p} \,] \geq [\, \overline{\mathbb{Z}_p}[\theta] : \overline{\mathbb{Z}}_p \,] = deg \overline{f_1}(x) = deg f_1(x),$$

which implies $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is unramified. □

In fact, $\overline{O_K}$ is the finite extension of the finite field $\overline{\mathbb{Z}_p}$ with dimension n and hence we can consider $\overline{O_K}$ as a splitting field of $x^{p^n} - x$ over $\overline{\mathbb{Z}_p}$, which is the unique extension of degree n. Hence we have a more description of K by discussing $\overline{O_K}/\ \overline{\mathbb{Z}_p}$.

THEOREM 2.2.3. *There is exactly one unramified extension* K_f^{un} *of* $\mathbb{Q}_p$ *of degree* f, *and it can be obtained by adjoining a primitive* $(p^f - 1)th$ *root of unity. Furthermore* $K_f^{un}/\mathbb{Q}_p$ *is cyclic.*

Proof. See [**2**, p.67] proposition. □

Theorem 2.2.3 tell us any unramified extension of $\mathbb{Q}_p$ of given degree is a cyclic extension and is unique . Furthermore the extension is of a very special type which is obtained by adjoining a primitive mth root, where m is related to its degree.

2.3. Totally ramified extensions of $\mathbb{Q}_p$

In this section we want to discuss characters of totally ramified extension of given degree and find polynomials which can generate these totally ramified extensions.

Let K be a totally ramified extension of $\mathbb{Q}_p$ of degree n and π be a prime element of K, then K= $\mathbb{Q}_p(\pi)$ and $O_K = \mathbb{Z}_p(\pi)$([**1**], p.47). Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$= Irr($\pi$, $\mathbb{Q}_p$), then by $f(\pi)$=0 we have

$$\upsilon_p(\pi^n) = \upsilon_p(a_{n-1}\pi^{n-1} + \cdots + a_0)$$

$$\geq \min_{0\leq i\leq n-1}\{\upsilon_p(a_i) + \frac{i}{n}\}.$$

Because $\upsilon_p(a_i) + \frac{i}{n}$ are all distinct,

$$1 = n\upsilon_p(\pi) = \min_{0\leq i\leq n-1}\{\upsilon_p(a_i) + \frac{i}{n}\},$$

which implies $\upsilon_p(a_i) \geq 1$ and $\upsilon_p(a_0) = 1$. For this kind of $f(x)$, we give a definition as follows:

Definition 2.3.1. A polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ over $\mathbb{Z}_p$ is called an *Eisenstein polynomial* if $a_0, \cdots, a_{n-1} \in M_p$, $a_0 \notin M_p^2$.

In lemma 2.3.2 we have the relation between Eisenstein polynomials and totally ramified extensions of $\mathbb{Q}_p$.

THEOREM 2.3.2. *Let $f(x)$ be an Eisenstein polynomial of degree n. Then $f(x)$ is irreducible over $\mathbb{Q}_p$. Let α be a root of $f(x)$, then $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is a totally ramified extension of degree n. Conversely, if K is a totally ramified extension of $\mathbb{Q}_p$ with a prime element π, then $Irr(\pi, \mathbb{Q}_p)$ is an Eisenstein polynomial.*

Proof. See [**1**] Proposition 3.6. □

Recall that we call a finite extension of $\mathbb{Q}_p$ is tamely ramified if its ramification index is not divisible by p. In the next lemma we have a more precise description of polynomials that can be used to get a totally and tamely ramified extension of dimension n.

PROPOSITION 2.3.3. *Let $K/\mathbb{Q}_p$ be a totally and tamely ramified extension of degree n. Then $K = \mathbb{Q}_p(\alpha)$ with a prime element α which satisfies the equation $x^n - a_0 p = 0$ for $a_0 \in U_p$. Conversely, if $p \nmid n$, then for any root α of $x^n - a_0 p$, $a_0 \in U_p$, $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is totally and tamely ramified of degree n.*

Proof. See[**1**, p.53], Proposition 3.5. □

By theorem 2.3.2 and proposition 2.3.3 we conclude that all totally ramified extensions of $\mathbb{Q}_p$ can be constructed by adjoining a root of an Eisenstein polynomial. Furthermore if its degree is not divisible by p, we can obtain it by adjoining a root of an Eisenstein polynomial with a special type.

2.4. Krasner's Lemma

In previous section we only know how to get a totally ramified extension of given degree. But even if two Eisenstein polynomials are distinct, they may generate the same extension. In fact we are interested in how many totally ramified extension of $\mathbb{Q}_p$ of given degree. In this section we will define a metric between two irreducible polynomials and connect Krasner's Lemma with metric of polynomials.

First, Krasner's Lemma tell us if an element in $\mathbb{Q}_p^{alg}$ is close enough to another then the two extensions obtained by adjoining these two elements, respectively, are the same.

LEMMA 2.4.1. (*Krasner's Lemma*). *Let $a, b \in \mathbb{Q}_p^{alg}$, and assume that b is chosen closer to a than all conjugates a_i of a ($a_i \neq a$), which means $|b-a|_p < |a_i - a|_p \ \forall\ a_i$. Then $\mathbb{Q}_p(a) \subset \mathbb{Q}_p(b)$.*

Proof. See [**2**, p.69]. □

But a root of a polynomial is not easy to describe. Hence we want to use Krasner's Lemma to find a method only related with coefficients of Eisenstien polynomials. Next we want to define a metric on set of all irreducible polynomials to help us reaching our goal.

For an irreducible polynomial $f(x)$ over $\mathbb{Q}_p$ of degree n, fix α a root of $f(x)$, let $g(x)$ be any other irreducible polynomial of degree n such that

$$|g(\alpha)|_p < (\min_{2\leq i\leq n}\{|\alpha - \alpha_i|_p\})^n.$$

Choose β be chosen among roots of $g(x)$ such that $|\beta - \alpha|_p$ is minimal. Then

$$|g(\alpha)|_p = \prod_{i=1}^{n} |\beta_i - \alpha|_p \geq (|\beta - \alpha|_p)^n ,$$

and hence

$$|\beta - \alpha|_p < \min_{2 \leq i \leq n} \{|\alpha - \alpha_i|_p\}.$$

By Krasner's Lemma we can conclude that $\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$. But $\mathbb{Q}_p(\alpha)$ and $\mathbb{Q}_p(\beta)$ have the same degree over $\mathbb{Q}_p$, hence $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. By this observation we define a metric on the set of all irreducible polynomials of $\mathbb{Q}_p$ of degree n.

For $f(x)$ and $g(x)$ are two irreducible polynomials over $\mathbb{Q}_p$ of degree n we define $|f - g|_p = |f(\beta)|_p$, where β is a root of $g(x)$. Let β' be another root of $g(x)$, and let F be the splitting field of $g(x)$ over $\mathbb{Q}_p$. Hence we can find $\sigma \in Gal(F/\mathbb{Q}_p)$ such that $\sigma(\beta) = \beta'$. Then we have

$$|f(\beta)|_p = |\sigma(f(\beta))|_p = |f(\sigma(\beta))|_p = |f(\beta')|_p.$$

Hence $|f - g|_p$ does not depend on the choice of β.

Now we will show $|f - g|_p = |g - f|_p$. Consider

$$|f(\beta)|_p^n = \prod_{i=1}^{n} |f(\beta - i)|_p = \prod_{i,j=1}^{n} |\beta_i - \alpha_j|_p,$$

where β_i, α_j are roots of $f(x)$ and $g(x)$, respectively. Thus for any root α of $g(x)$, we have $|f(\beta)|_p = |g(\alpha)|_p$.

It is easy to check that $|\cdot|_p$ satisfies $|f - h|_p \leq \max\{|f - g|_p, |g - h|_p\}$, where $f(x)$, $g(x)$ and $h(x)$ are irreducible polynomials of degree n over $\mathbb{Q}_p$ and satisfies the condition $|f - g|_p = 0$ if and only if $f(x) = g(x)$.

DEFINITION 2.4.2. Let $f(x)$, $g(x)$ be two irreducible polynomials of $\mathbb{Q}_p$ of degree n. Define $|f-g|_p := |f(\beta)|_p$, where β is a root of $g(x)$. Then $|f-g|_p$ is well-defined and defines a metric on the set of all irreducible polynomials of degree n.

LEMMA 2.4.3. *Let $f(x)$, $g(x)$ be two irreducible polynomials of $\mathbb{Q}_p$ of degree n.Let $\alpha = \alpha_1, \cdots, \alpha_n$ be roots of $f(x)$, and β be chosen among the roots of $g(x)$ such that $|\beta - \alpha|_p$ is minimal. Then*

$$|f-g|_p = \prod_{i=1}^{n} \max\{|\beta-\alpha|_p, |\alpha-\alpha_i|_p\}.$$

Proof. See [**5**, p.1643]. □

By the observation in the beginning of this section we have a conclusion written as follows:

LEMMA 2.4.4. *Let $f(x)$ be an irreducible polynomial over $\mathbb{Q}_p$ of degree n, and let α be a root of $f(x)$, let $g(x)$ be any other irreducible polynomial of degree n such that*

$$|f-g|_p < (\min_{2\le i\le n}\{|\alpha-\alpha_i|_p\})^n.$$

, where α_i are another roots of $f(x)$. Choose β be chosen among roots of $g(x)$ such that $|\beta-\alpha|_p$ is minimal. Then $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$.

PROPOSITION 2.4.5. *Let $f(x)$ be an irreducible polynomial over $\mathbb{Q}_p$ of degree n. Let $\delta = \min_{i\neq j}\{|\alpha_i - \alpha_j|_p\}$. Let $g(x)$ is another irreducible polynomial over $\mathbb{Q}_p$ of degree n satisfying $|f-g|_p < \delta^n$, then for every root α_i of $f(x)$*

there is precisely one root β_i of $g(x)$ such that $|\alpha_i - \beta_i|_p < \delta$, which implies $\mathbb{Q}_p(\alpha_i) = \mathbb{Q}_p(\beta_i)$

Proof. Let β be a root of $g(x)$. Because

$$|f - g|_p = |f(\beta)|_p = \prod_{i=1}^{n} |\alpha_i - \beta|_p < \delta^n = (\min_{i \neq j}\{|\alpha_i - \alpha_j|_p\})^n.$$

Hence there exists a root α_k such that $|\alpha_k - \beta|_p < \delta$. If there is another root $\alpha' \neq \alpha_k$ of $f(x)$ satisfying $|\alpha' - \beta|_p < \delta$, then

$$|\alpha' - \alpha_k|_p \leq \max\{|\alpha_k - \beta|_p, |\alpha' - \beta|_p\} < \delta,$$

contradiction. Hence there is precisely one root α_k of $f(x)$ satisfying $|\alpha_k - \beta|_p < \delta$ for fixed β. □

Denote the set of all Eisenstien polynomials of degree n by E_n. In fact, $|f - g|_p$ is easily calculated using the following lemma when $f(x)$, $g(x)$ are elements in E_n.

LEMMA 2.4.6. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ are two Eisenstien polynomials over $\mathbb{Z}_p$, then*

$$|f - g|_p = \max_{0 \leq i \leq n-1}\{p^{-(\frac{i}{n})}|a_i - b_i|_p\}.$$

Proof. Let β be a root of $g(x)$, then

$$|f - g|_p = |f(\beta)|_p = |f(\beta) - g(\beta)|_p = |\sum_{i=0}^{n-1}(a_i - b_i)\beta^i|_p.$$

Since β is a prime element, $|\beta|_p = p^{-\frac{1}{n}}$. Thus in above sum all the terms have different norms. It follows that $|f - g|_p$ is the maximal of those. □

Next we define the discriminant of a polynomial and of a finite extension of $\mathbb{Q}_p$.

2.5. Discriminant

DEFINITION 2.5.1. Let K be a finite extension of $\mathbb{Q}_p$ with $\{x_1, \cdots, x_n\}$ as a basis of K over $\mathbb{Q}_p$. Set $\Delta(x_1, \cdots, x_n) := \det[\ Tr_{K/\mathbb{Q}_p}(x_i x_j)\ ]$, where $[\ Tr_{K/\mathbb{Q}_p}(x_i x_j)\ ]$ is a $n \times n$ matrix with entries $Tr_{K/\mathbb{Q}_p}(x_i x_j)$. If $x_i \in O_K$ for all i, we have $\Delta(x_1, \cdots, x_n) \in \mathbb{Z}_p$. If we let $x_1, \cdots, x_n$ range over all bases of K over $\mathbb{Q}_p$ that lie in O_K these $\Delta(x_1, \cdots, x_n)$ generate an ideal Δ_K which we call the *discriminant* (ideal) of K over $\mathbb{Q}_p$.

When $K/\mathbb{Q}_p$ is totally ramified, the discriminant of K is of a special type.

LEMMA 2.5.2. *Let K be a totally ramified extension of $\mathbb{Q}_p$ of degree n. Then $O_K = \mathbb{Z}_p(\pi)$, where π is a prime element of K and hence Δ_K is a principal ideal with generator $\Delta(\pi)$, where $\Delta(\pi) = \Delta(1, \pi, \cdots, \pi^{n-1})$.*

Proof. See [**1**] and [**6**]. □

DEFINITION 2.5.3. Let $f(x)$ be a polynomial over $\mathbb{Q}_p$ of degree n with n distinct roots $\alpha_1, \alpha_2, \cdots, \alpha_n$ in $\mathbb{Q}_p^{alg}$. Let $D = \prod_{i<j}(\alpha_i - \alpha_j)$; the *discriminant* of $f(x)$ is the element $\Delta_f = D^2$.

In fact, there is a formula to calculate a discriminant of an irreducible polynomial of given degree.

PROPOSITION 2.5.4. *Let $f(x)$ be an irreducible polynomial over $\mathbb{Q}_p$ of degree n, and let $K = \mathbb{Q}_p(\alpha)$, where α is a root of $f(x)$. Then*

$$\Delta(\alpha) = \Delta(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}_p}(f'(\alpha)).$$

Proof. See[**6**, p.39]. □

Now we want to discuss a relation between discriminant of an Eisenstien polynomial $f(x)$ and discriminant of a totally ramified extension of $\mathbb{Q}_p$ generated by adjoining a root of $f(x)$.

COROLLARY 2.5.5. *Let K be a totally ramified extension of $\mathbb{Q}_p$ of degree n and let $f(x) = Irr(\pi, \mathbb{Q}_p)$, then $\Delta(\pi) = \Delta_f$ and hence $\Delta_K = M_p^{\upsilon_p(\Delta_f)}$.*

Proof. It follows from proposition 2.5.2 and 2.5.4. □

Now we know that any two Eisenstien polynomial $f(x)$, $g(x)$ with different discriminant (i.e., $\upsilon_p(\Delta_f) \neq \upsilon_p(\Delta_g)$) must generate different totally ramified extensions but two distinct totally ramified extension may have the same discriminant. Hence we will focus on finding all totally ramified extensions of $\mathbb{Q}_p$ with fixed discriminant.

But for fix n, given $m \in \mathbb{N}$, there does not necessarily exist a totally ramified extension of $\mathbb{Q}_p$ of degree n with discriminant M_p^m. Next we offer a method to check existence of totally ramified extensions of degree n and discriminant M_p^{n+j-1}.

Fix n. For any integer j we write $j = an + r_j$, where $0 \leq r_j < n$. Then we say j satisfies *Ore's condition* if

$$\min\{\upsilon_p(r_j)n, \upsilon_p(n)n\} \leq j \leq \upsilon_p(n)n.$$

PROPOSITION 2.5.6. (*Ore's conditions*). *Fix n and given an integer j. Then there exist a totally ramified extensions of $\mathbb{Q}_p$ of degree n and discriminant M_p^{n+j-1} if and only if j satisfies Ore's condition.*

Proof. See [**7**] □

REMARK 1. For fixed n, we have some properties with j which satisfies *Ore'sconditions* with respect to n.

(1) $p \nmid n$. Then we have $\upsilon_p(n) = 0$ and hence $\upsilon_p(r_j) \geq \upsilon_p(n)$ for $j = an + r_j$, where $0 \leq r_j < n$. This implies if j satisfies *Ore'sconditions*, then j must be $\upsilon_p(n)n$ and hence equals to 0. Conversely, if $j = 0$, then j satisfies *Ore'sconditions*. We conclude that all totally and tamely ramified extensions of $\mathbb{Q}_p$ with degree n have the same (field) discriminant M_p^{n-1}.

(2) $p \mid n$. Then $\upsilon_p(n) \geq 1$. For $j = an + r_j$, where $0 \leq r_j < n$ we classify the case to remainder. If $r_j = 0$, we have $\upsilon_p(r_j) = \infty$ and hence j must be $\upsilon_p(n)n$. We conclude that if j satisfies *Ore'sconditions*, then $n \mid j$ if and only if $j = \upsilon_p(n)n$.

Ore'sconditions can help us classify all totally ramified extensions of $\mathbb{Q}_p$ of degree n to discriminant. Hence if we want to calculate the number of all totally ramified extensions of $\mathbb{Q}_p$ of degree n, we just need to calculate

the number of all totally ramified extensions of $\mathbb{Q}_p$ of degree n with (field) discriminant M_p^{n+j-1} for all j satisfying $Ore'sconditions$.